UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/841,503	04/24/2001	Richard Alan Dayan	RPS9 2001 0011	5669

7590 03/28/2005

IBM Corporation
Personal and Printing Systems Group
Dept. 9CCA/Bldg. 002-2
P.O. Box 12195
Research Triangle Park, NC 27709

EXAMINER	
HENNING, MATTHEW T	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 03/28/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/841,503	DAYAN ET AL.	
	Examiner	Art Unit	
	Matthew T Henning	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *29 November 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-36* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-36* is/are rejected.

7)☒ Claim(s) *26* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *24 April 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

This action is in response to the communication filed on 11/29/2004.

DETAILED ACTION

1. All rejections and objections not specifically set forth below have been withdrawn.

2. Claims 1-36 have been examined.

Title

3. The title of the invention is acceptable.

Priority

4. No claim for priority has been made for this application.

5. The effective filing date for the subject matter defined in the pending claims in this application is 04/24/2001.

Information Disclosure Statement

6. The information disclosure statement (IDS) submitted on 04/24/2001 is in compliance with the provisions of 37 CFR 1.97. Accordingly, the examiner is considering the information disclosure statement.

Drawings

7. The drawings filed on 04/24/2001 are acceptable for examination proceedings.

Claim Objections

8. Claim 26 is objected to because of the following informalities: Line 14 recites "said formation" which does not make sense with the claim. As such, the examiner will assume the claim was meant to read "said information". Appropriate correction is required.

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. Claims 1- 4,13-19, and 26-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gafken (US Patent Number 6,026,016), and further in view of Hasbun et al. (U.S. Patent Number 6,088,759) hereinafter referred to as Hasbun.

Regarding claim 1, Gafken disclosed a method for updating a protected partition within a hard drive of a computing system, wherein said method comprises (See Gafken Fig. 5): starting execution of an initialization program in a processor within said computing system in response to turning on electrical power within said computing system (See Gafken Col. 3 Paragraph 2 Lines 1-4); determining whether an update partition file is stored in non-volatile storage (See Gafken Col. 5 Paragraph 5) within said computing system for subsequently updating said protected partition (See Gafken Col. 13 Paragraphs 4 and 7); after determining that said update partition is stored within said computing system for updating said protected partition, writing a portion of said update partition file to said protected partition (See Gafken Col. 13 Paragraph 8); and locking said protected partition to prevent further modification of information stored within said protected partition (See Gafken Col. 13 Paragraph 9 – Col. 14 Paragraph 1), but failed to disclose overwriting similar parts and appending new parts.

Hasbun teaches that a bios update can be allocated into virtual blocks so that the blocks can be updated individually without having to erase the entire memory first (See Hasbun Col. 5

Paragraph 6 – Col. 6 Paragraph 2). Hasbun also teaches that new blocks should be allocated from existing free memory (See Hasbun Col. 7 Paragraph 2).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Hasbun to the bios updating system of Gafken by updating each update part one at a time. This would have been obvious because the ordinary person skilled in the art would have been motivated to provide a safe method for updating a bios without risking loss of the entire bios in the event of a power failure.

11. Regarding claim 2, the combination of Gafken and Hasbun disclosed that a flag bit is set in non-volatile storage within said computing system when said update partition file is stored at a predetermined location in non-volatile storage within said computing system (See Gafken Col. 13 Paragraphs 3-4), and determining whether said update partition is stored within said computing system for updating said protected partition is performed by determining whether said flag bit is set (See Gafken Col. 13 Paragraph 7 and Fig. 5 Step 550).

12. Regarding claim 3, the combination of Gafken and Hasbun disclosed that after determining that said update partition file is stored within said computing system for updating said protected partition, verifying whether said update partition file has been generated by a trusted server system, and said portion of said update partition is written to said protected partition only following verification that said update partition file has been generated by a trusted server system (See Gafken Col. 12 Paragraph 6 – Col. 13 Paragraph 1 and Figure 6).

13. Regarding claim 4, the combination of Gafken and Hasbun disclosed that verification that said update partition file has been generated by said trusted server system includes: forming a first message digest by applying a hash algorithm to a portion of said update partition file;

forming a second message digest by decrypting a digital signature within said update partition file using a public key of said trusted server system; and determining that said first and second message digests are identical (See Gafken Col. 12 Paragraph 7 Line 10 – Col. 13 Line 2).

14. Regarding claim 13, the combination of Gafken and Hasbun disclosed a method for updating a protected partition within a hard drive of a client computing system, wherein said method comprises: generating an update partition file within a server (See Gafken Col. 12 Paragraph 7 – Col. 13 paragraph 1, wherein it was inherent that the server created the image by signing it in order for the server to be verified through digital signatures); transferring said update partition file from said server to said client computing system (See Gafken Col. 12 Paragraph 5); storing said update partition file in non-volatile storage within said client computing system (See Gafken Col. 5 Paragraph 5); starting execution of an initialization program in a processor within said client computing system in response to turning on electrical power within said client computing system (See Gafken Col. 3 Paragraph 2 Lines 1-4); determining that said update partition file is stored in non-volatile storage within said client computing system (See Gafken Col. 13 Paragraphs 4 and 7); writing a portion of said update partition file to said protected partition (See Gafken Col. 13 Paragraph 8); and locking said protected partition to prevent further modification of information stored within said protected partition (See Gafken Col. 13 Paragraph 9 – Col. 14 Paragraph 1). The combination of Gafken and Hasbun further disclosed comparing information stored in said protected partition with information within said update partition file; when a matching portion of said information stored in said protected partition is found to be similar to said entry, said matching portion is overwritten with said entry if space around said matching portion is sufficient, and when a

matching portion of said information stored in said protected partition is not found to be similar to said entry, said entry is appended to said information stored in said protected partition if space within said protected partition is sufficient (See the rejection of claim 1 above).

15. Regarding claim 14, the combination of Gafken and Hasbun disclosed that the update partition file is transferred from said server to said client computing system by means of electrical signals transmitted through a public switched telephone network (See Gafken Col. 4 Paragraph 7 wherein it was inherent that the update file was received through the wireless transmitter, and therefore through a public switched telephone network).

16. Regarding claim 15, the combination of Gafken and Hasbun disclosed that update partition file is transferred from said server to said client computing system by means of electrical signals transmitted over a local area network (See Gafken Col. 12 Paragraph 5).

17. Regarding claim 16, the combination of Gafken and Hasbun disclosed that transferring said update partition file from said server to said client computing system includes: writing said update partition file to a removable computer readable medium from said server; transporting said removable computer readable medium from said sever to said client computing system; and reading said update partition file from said removable computer readable medium into said client computing system (See Gafken Col. 12 Paragraph 5 wherein it was inherent that the image was stored to a floppy disk and retrieved from the floppy disk in order for the image to have been obtained through a floppy drive).

18. Claim 17 is rejected for the same reasons as claim 2 above.

19. Claim 18 is rejected for the same reasons as claim 3 above.

20. Regarding claim 19, the combination of Gafken and Hasbun disclosed the use of digital signatures to verify the origin of the update file (See Gafken Col. 12 Paragraph 7 – Col. 13 Paragraph 1).

21. Claim 26 recites a computer system comprising: a processor executing an initialization program in response to power being turned on in said computer program (See Gafken Fig. 1 Element 110); a hard drive having a protected partition blocked during execution of an initialization program to prevent changing information stored within said protected partition (See Fig. 1 Element 130); non-volatile storage storing an update partition data structure for modifying contents of said protected partition and said initialization program, wherein said initialization program executing within said processor determines that said update partition data structure is stored in said non-volatile storage, writes a portion of said update partition data structure to said protected partition, and locks said protected partition to prevent further modification of information stored within said protected partition (See rejection of claim 1 above). The combination of Gafken and Hasbun further disclosed comparing information stored in said protected partition with information within said update partition file; when a matching portion of said information stored in said protected partition is found to be similar to said entry, said matching portion is overwritten with said entry if space around said matching portion is sufficient, and when a matching portion of said information stored in said protected partition is not found to be similar to said entry, said entry is appended to said information stored in said protected partition if space within said protected partition is sufficient (See the rejection of claim 1 above).

22. Claim 27 is rejected for the same reasons as claim 2 above.

23. Claim 28 is rejected for the same reasons as claim 3 above.

24. Claims 5, 6, 20-21, and 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Gafken and Hasbun as applied to claims 3 and 18 above, and further in view of Schneier ("Applied Cryptography").

Regarding claims 5 and 20, the combination of Gafken and Hasbun disclosed the use of digital signatures, including public and private keys, in order to verify that a valid server generated the boot image (See Gafken Col. 12 Paragraph 7 – Col. 13 Paragraph 1), but the combination of Gafken and Hasbun failed to disclose the use of a password in the signature. However, the combination of Gafken and Hasbun did disclose the use of password challenges.

Schneier teaches that providing a random number (password), supplied by a receiver to a sender, in a digital signature of the sender, causes the signature to be undeniable and therefore secure (See Schneier Page 81).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Schneier to the validation signatures of the combination of Gafken and Hasbun by providing predetermined random number in the signature of the update image. This would have been obvious because the ordinary person skilled in the art would have been motivated to provide protection against illicitly signed updates.

25. Regarding claims 6 and 21, the combination of Gafken, Hasbun, and Schneier disclosed that the data includes said version of said setup password appended to a portion of said update partition file (See rejection of claim 5 above), said algorithm is a hash algorithm generating a message digest (See Gafken Col. 12 Paragraph 7 – Col. 13 Paragraph 1), and verifying that said update partition file has been generated by said trusted server system includes applying said hash

algorithm to said setup password stored within said computing system appended to a portion of said update partition file to generate a first version of a message digest and comparing said first version of said message digest with a second version of said message digest obtained by signing said encrypted portion of said update partition file (See Gafken Col. 12 Paragraph 7 – Col. 13 Paragraph 1).

26. Regarding claim 33, it would have been inherent that the random number (password) was stored for access, at least temporarily, at the server in order for the server to have used the password to sign the update.

27. Claims 7, 8, 11, 22, 23, and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Gafken and Hasbun as applied to claims 1, 13, and 28 above, and further in view of Hayashi et al. (US 2001/0039651 A1) hereinafter referred to as Hayashi.

Regarding claims 7, 22, and 29, the combination of Gafken and Hasbun disclosed digitally signing the update file and verifying the signature prior to updating the partition (See Gafken Col. 12 Paragraph 7 – Col. 13 Paragraph 1), but the combination of Gafken and Hasbun failed to disclose encrypting portions of the file separately and verifying each portion individually.

Hayashi teaches a method for providing a variety of software safely by breaking the file into pieces and decrypting each piece separately (See Hayashi Page 1 Col. 2 Paragraphs 3-10).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Hayashi to the updating system of the combination of Gafken and Hasbun by encrypting parts of the file separately from the other parts. This would have been obvious because the ordinary person skilled in the art would have been motivated to

provide users with customized software without imposing too much of a load on the provider. In this combination, it would also be obvious that each block contained information to be stored in a different location from the other blocks. This would have been obvious because the ordinary person skilled in the art would have been motivated not perform unnecessary computation during the update.

28. Regarding claim 8, the combination of Gafken, Hasbun, and Hayashi disclosed forming a first message digest by applying a hash algorithm to said entry, and forming a second message digest by signing said encrypted element associated with said entry using a public key of said trusted server system, and determining that said first and second message digests are identical (See Gafken Col. 12 Paragraph 7 Line 10 – Col. 13 Line 2).

29. Regarding claim 11, the combination of Gafken, Hasbun, and Hayashi disclosed that information stored in said protected partition is compared to each entry in said plurality of entries within said update partition, when a matching portion of said information stored in said protected partition is found to be similar to said entry, said matching portion is overwritten with said entry if space around said matching portion is sufficient, and when a matching portion of said information stored in said protected partition is not found to be similar to said entry, said entry is appended to said information stored in said protected partition if space within said protected partition is sufficient (See the rejection of claim 1 above).

30. Regarding claim 23, the combination of Gafken, Hasbun, and Hayashi disclosed that each encrypted element is formed in said server by applying a hash algorithm to said entry, forming a first message digest, and by signing said first message digest with a private key of said server; and verification that said entry has been generated by said server includes forming a second

message digest by applying a hash algorithm to said entry, forming a third message digest by signing said encrypted element associated with said entry using a public key of said server, and determining that said second and third message digests are identical (See Gafken Col. 12 Paragraph 7 Line 10 – Col. 13 Line 2).

31. Claims 9, 10, 24-25, 30-32, and 34-35 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Gafken, Hasbun, and Hayashi as applied to claims 7, 22 and 29 above, and further in view of the combination of Schneier.

Regarding claim 9, Gafken, Hasbun and Hayashi disclosed the use of digital signatures, including public and private keys, in order to verify that a valid server generated the boot image parts (See Gafken Col. 12 Paragraph 7 – Col. 13 Paragraph 1), but Gafken, Hasbun, and Hayashi did not disclose the use of a password in the signature. However, Gafken, Hasbun and Hayashi did disclose the use of password challenges (See Gafken Col. 12 Paragraph 7 – Col. 13 Paragraph 1).

Schneier teaches that providing a random number (password), supplied by a receiver to a sender, in a digital signature of the sender, causes the signature to be undeniable and therefore secure (See Schneier Page 81).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Schneier to the validation signatures of Gafken, and Hayashi by providing predetermined random number in the signatures of the update parts. This would have been obvious because the ordinary person skilled in the art would have been motivated to provide protection against illicitly signed update parts.

32. Regarding claim 10, the combination of Gafken, Hasbun, Hayashi, and Schneier disclosed that the data includes said version of said setup password appended to a said entry (See rejection of claim 5 above), said algorithm is a hash algorithm generating a message digest, and verifying that said entry has been generated by said trusted server system includes applying said hash algorithm to said setup password stored within said computing system appended said entry to generate a first version of a message digest and comparing said first version of said message digest with a second version of said message digest obtained by signing said encrypted element (See Gafken Col. 12 Paragraph 7 – Col. 13 Paragraph 1).

33. Regarding claim 24, the combination of Gafken, Hasbun, Hayashi, and Schneier disclosed that a setup password is stored in non-volatile storage within said client computing system; a copy of said setup password is stored in a database accessed by said Server (See rejection of claim 5 above); said encrypted element of said update partition file is prepared in said server by signing, with a private key of said server, a result of the application of an algorithm to data including said copy of said setup password', and verification within said client computing system that said entry has been generated by said server includes signing said encrypted element associated with said entry with said public key of said server (See Gafken Col. 12 Paragraph 7 – Col. 13 Paragraph 1).

34. Claim 25 is rejected for the same reasons as claim 10 above as applied to claim 24 above.

35. Regarding claim 30, the combination of Gafken, Hasbun, Hayashi, and Schneier disclosed that the non-volatile storage additionally stores a setup password, and each said encrypted element includes a digital signature signed by said trusted server system, wherein said digital signature is formed by applying a hash algorithm to an entry associated with said

encrypted element to form a message digest and by signing said message digest with a private key of said trusted server system (See Gafken Col. 12 Paragraph 7 – Col. 13 Paragraph 1).

36. Claim 31 is rejected for the same reasons as claim 10 above.

37. Claim 32 is rejected for the same reasons as claim 10 above and further because Gafken disclosed a processor (See Gafken Fig. 1 Element 110).

38. Regarding claims 34 and 35, it would have been inherent that the random number (password) was stored for access, at least temporarily, at the server in order for the server to have used the password to sign the update.

39. Claim 36 is rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Gafken, Hasbun, Hayashi, and Schneier as applied to claim 32 above, and further in view of the combination of Galasso et al. (US Patent Number 6,148,387), hereinafter referred to as Galasso.

The combination of Gafken, Hasbun, Hayashi, and Schneier disclosed sending a BIOS update from a server to a client based on a client update request (See Gafken Col. 13 Paragraph 2), but failed to disclose authenticating the BIOS update request at the server.

Galasso teaches that BIOS service requests should be signed using a private key and the request should be verified using the public key associated with the private key (See Galasso Col. 2 Lines 36-42).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Galasso in the BIOS update system of Gafken, Hasbun, Hayashi, and Schneier. This would have been obvious because the ordinary person skilled in the art would have been motivated to ensure the integrity of the update request.

In this combination, it would have been inherent that the server had access to the public key in order for the server to have verified the signature in the request.

40. Claim 12 is rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Gafken and Hasbun as applied to claim 1 above, and further in view of Schmidt (U.S. Patent Number 5,826,015).

The combination of Gafken and Hasbun disclosed a secure bios updating system (See rejection of claim 1 above) but failed to disclose requiring a user to input a password to unlock the bios write capabilities. However, Gafken and Hasbun did disclose the use of password challenges (See Gafken Col. 12 Paragraph 7 – Col. 13 Paragraph 1).

Schmidt teaches that in order to remotely upgrade a bios, an administrator password should be provided in order to unlock the partition (See Schmidt Fig. 9 and abstract).
It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Schmidt to the bios updating system of Gafken by requiring a correct password to be entered in order to unlock the bios altering capabilities. This would have been obvious because the ordinary person skilled in the art would have been motivated to protect the current bios from accidental or illicit alterations.

Response to Arguments

41. Applicant's arguments filed 11/29/2004 have been fully considered but they are not persuasive.

42. Applicant argues primarily that:

a. Gafken did not disclose the new limitations in the amended claims 1, 13, and 26.

b. Gafken did not disclose writing the protected partition to a predetermined location.

c. Gafken did not disclose providing for the writing of information to various locations that may not be contiguous.

d. Gafken did not disclose that the entries included information to be stored in different locations.

e. The examiner provided a different reason to combine the references applied to claim 11 than the applicant.

43. Applicant's argument a. with respect to claims 1, 13, and 26 have been considered but are moot in view of the new ground(s) of rejection. The examiner points out that the new limitations of claims 1, 13, and 26 are very similar to claim 11, but are not the same as claim 11 and therefore, a new grounds of rejection is proper. Furthermore, the new limitations of claims 1, 13, and 26 do not include the limitations of claim 7. Therefore, these claims are new and have not been previously presented.

44. Applicant's argument b. with respect to claims 2, 17, and 27 have been considered but are not considered persuasive. As pointed to above, Gafken disclosed storing the code updates in a predetermined location (See Gafken Col. 13 Paragraph 3).

45. The examiner has maintained the rejections presented above with regards to claims 3, 4, 14-16, 18, and 28 because the argument a. was not persuasive.

46. The examiner has maintained the rejections presented above with regards to claims 5, 6, 20, and 21 because the argument a. was not persuasive.

47. Applicant's argument c. with respect to claims 7, 8, 22, 23, and 29 have been considered and are not considered persuasive. In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., providing for the writing of information to various locations that may not be contiguous) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). As such, the examiner is maintaining the rejection presented above with regards to claims 7, 8, 22, 23, and 29.

48. Applicant's argument d. with respect to claims 7, 22, 29, 31, and 32 has been considered but is not considered persuasive. If each block did not contain code to be stored in its own separate location, at least some of the code would be overwritten by other code during the update. This would have been a waste of processing and time because the overwritten code would not be used. Because of this, it would have been obvious to only provide code that would be written to its own location. Because of this, the examiner is maintaining the rejection presented above with regards to claims 7, 22, and 29.

49. The examiner has maintained the rejections presented above with regards to claims 8 and 23 because the arguments a. c. and d. were not persuasive.

50. The examiner has maintained the rejections presented above with regards to claims 9, 10, 24, and 30 because the arguments a. c. and d. were not persuasive.

51. Claim 25 has been addressed accordingly above, and is made final because no claim has been presented with the limitations of claim 25 prior to the amendment filed 11/29/2004.

52. In response to applicant's argument that e., the fact that applicant has recognized another advantage which would flow naturally from following the suggestion of the prior art cannot be the basis for patentability when the differences would otherwise be obvious. See *Ex parte Obiaya*, 227 USPQ 58, 60 (Bd. Pat. App. & Inter. 1985). Therefore, the examiner has maintained the rejection presented above with regards to claims 1, and 11 above.

53. The examiner has maintained the rejections presented above with regards to claim 12 because the arguments a. c, d, and e. were not persuasive.

54. All new claims have been addressed above.

Conclusion

55. Claims 1-36 have been rejected.

56. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew T Henning whose telephone number is (571) 272-3790. The examiner can normally be reached on M-F 8-4.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Matthew Henning
Assistant Examiner
Art Unit 2131
3/21/2005

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100